IN THE UNITED STATES BANKRUPTCY COURT
FOR THE DISTRICT OF DELAWARE

In re	Chapter 11
FTX TRADING LTD., *et al.*,	Case No. 22-11068-JTD
Debtors.[1]	Jointly Administered
	Re: D.I. 1137

DECLARATION OF PHILIP JAMES IN SUPPORT OF THE AD HOC COMMITTEE OF NON-US CUSTOMERS OF FTX.COM'S MOTION TO FILE UNDER SEAL THE VERIFIED STATEMENT OF EVERSHEDS SUTHERLAND (US) LLP AND MORRIS, NICHOLS, ARSHT & TUNNELL LLP PURSUANT TO BANKRUPTCY RULE 2019

I, Philip James, declare under penalty of perjury:

1. I am a member, otherwise referred to as a "partner," of Eversheds Sutherland (International) LLP's (the "Firm") Global Privacy and CyberSecurity Group. I am based at the Firm's London office, which is located at 1 Wood Street, London, EC2V 7WS, United Kingdom.

2. I counsel clients on UK and EU GDPR, data protection, privacy, cybersecurity and reputation management. I specialize in the Technology, Media and Financial Services sectors and am a member of the Firm's Technology in Financial Services (and associated Distributed Ledger Technology) sub-sector group. I have over twenty years' experience in privacy, data protection, technology, and media law.

3. I submit this Declaration in support of the *Ad Hoc Committee of Non-US*

[1] The last four digits of FTX Trading Ltd.'s and Alameda Research LLC's tax identification numbers are 3288 and 4063 respectively. Due to the large number of debtor entities in these Chapter 11 Cases, a complete list of the Debtors and the last four digits of their federal tax identification numbers is not provided herein. A complete list of such information may be obtained on the website of the Debtors' claims and noticing agent at https://cases.ra.kroll.com/FTX.

Customers' Motion to File Under Seal the Verified Statement of Eversheds Sutherland (US) LLP and Morris, Nichols, Arsht & Tunnell LLP Pursuant to Bankruptcy Rule 2019 (the "Motion"). I have reviewed an unredacted version of the *Verified Statement of Eversheds Sutherland (US) LLP and Morris, Nichols, Arsht & Tunnell LLP Pursuant to Bankruptcy Rule 2019* (the "2019 Statement") and Motion in preparing this Declaration.

A. UK and EU Law

4. Upon information and belief, it is my understanding that each member of the Ad Hoc Committee of Non-US Customers of FTX.com (the "Ad Hoc Committee") is a customer that holds an account on the FTX.com exchange (each, a "Member"). As reflected in the 2019 Statement, each Member is also an entity or natural person domiciled outside the United States, including natural persons residing in the UK or EU countries. These Members' identity, privacy, and right to a private life and protection of personal information afforded under the EU Charter of Fundamental Rights (the "EU Charter") and the European Convention of Human Rights ("ECHR") is at risk if the Court requires that the names and addresses of these Members must be publicly disclosed.

5. EU and UK General Data Protection Regulations ("GDPR") underpin ECHR. GDPR protects the processing of personal data (i.e. personal information) via which natural living persons may be identified or identifiable—an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person and has extra-territorial reach, requiring compliance by entities worldwide that meet the requirements of Article 3 (these are drafted very broadly). In particular, the presumption is that

everyone has a right to privacy and the protection of their personal data unless a lawful basis, derogation or exception under GDPR applies. It is my understanding that the Court has recognized the potential impact of GDPR in this case by permitting the redaction of names, e-mail addresses, and addresses of any creditor or equity holder that is a natural person and is protected by GDPR *See* D.I. 545.

6. Whilst it is acknowledged that the United States Bankruptcy Code (the "Bankruptcy Code") has a presumption in favor of making records public, there is an equal and contrary presumption in favor of protecting Members' identity under GDPR, the EU Charter and ECHR.

7. I acknowledge and understand a need to demonstrate extraordinary circumstances to justify the redaction and/or withholding of Members' first and last names; however, if ever there was an extraordinary and exceptional set of circumstances, it is these cases.

B. Extraordinary Circumstances Exist In This Case

8. The magnitude and profile of the FTX cases is demonstrated by the media intervention, instigated by, amongst others, the New York Times, Bloomberg and the Financial Times (the "Media Intervention"). *See* D.I. 195, 196. This incredible level of the media interest indicates the likely impact and magnitude of distress, anxiety and loss of privacy that would be caused by disclosure of individual Members' first and last names.

9. It is generally accepted that the redaction of email addresses, contact details and postal addresses are reasonable in the circumstances; however, it is also the disclosure of Members' first and last names that remains a significant cause for concern.

10. For example, it is evident how easy it is for anyone, even those without any specialist investigative skills or experience, to find out a significant amount about a person simply by searching their name, using the "search" function on LinkedIn. By carrying out such a search,

it is possible to find out many personal details including: their contact details; current and/or previous employer; place of work; home town; interest groups; other contacts to whom that individual is connected; university; and higher education and school education. This does not factor in other forms of social media or use of sophisticated search engines or generative AI (artificial intelligence) applications, such as ChatGPT, offered by OpenAI. In the hands of a hacker, dark web crypto miner or expert, or investigative journalist, that first and last name becomes, on its own, the real and genuine opportunity to create a deep profile of a Member and his or her family, friends and contacts. This may likely result in a hacker attempting one of the many ways that thieves target cryptocurrency holders, including:

- Stealing an Online Wallet. The most common way to steal digital assets is by stealing a digital wallet. If a wallet holder's Personally Identifying Information is disclosed, the risk of theft is significantly heightened.
- Theft of Private Keys. A criminal could also use Personally Identifying Information in a variety of ways to trick a wallet holder into surrendering its private keys, including phishing emails, phone calls, and phony donation requests.
- Physical Robbery. Cryptocurrency holders have also been the victims of physical robbery. Holders can be forced to surrender hardware wallets, passwords, and other access credentials to online wallets. Sophisticated criminals easily determine the addresses of customers with only a name. Targeting of known holders of cryptocurrency to steal their wallets or keys is becoming increasingly common.
- SIM Swapping. "SIM swapping" occurs when a criminal gains access to a victim's cell phone account through an accomplice at a wireless provider. Because most providers of online wallets rely upon text messaging for security in password resets, a

criminal who has obtained a SIM-swapped device can effortlessly take over any such online wallet.

11. These risks are not something that the Bankruptcy Code, or anyone decades ago, anticipated. Moreover, it is not merited that, simply because a Member was a customer of FTX.com, their personal and private life should be exposed to the potentially intrusive journalism and investigation associated with the FTX cases (as well as the real risk of hacking attempts which may be likely to occur as a result).

C. The Fair Processing Notice Is Not Sufficient to Enable Disclosure

12. It is my understanding that Members' personal information was originally shared pursuant to an agreement that is governed by terms of service subject to English law. [Adv. Pro. 22-50514, D.I. 1, Ex. B]. In addition, Members signed up to a service provided by a corporation incorporated and registered in Antigua, and only available to customers outside of the United States. While FTX's privacy policy permits disclosure of Members' personal information to external third parties and for law enforcement or exercise of legal rights, it does not permit nor grant authority to publish Members' private information publicly. Obviously limited disclosure to external third parties is quite different than disclosure of Members' private information to the wider public, and, in particular, the media.

13. Personal information also constitutes private and confidential information governed by the law of tort and also by applicable common (or codified civil) law principles of privacy afforded in individuals pursuant to the relevant applicable UK and EU law—for instance, aside from GDPR, in the UK, where circumstances dictate that an individual has or had a reasonable expectation of privacy and/or confidentiality, and that information regarding that person's private life, private information or confidential information relating to that person's affairs are

subsequently disclosed in circumstances which are not justified (*i.e*. their disclosure is not in the public interest as that person has not necessarily done anything wrong or committed any wrongdoing or misdemeanor (in analogous US terminology)), that person may be able to bring a claim for privacy, misuse of private information and/or breach of confidence. In France, for example, privacy and a person's private life and protection of identity in this way is perhaps protected to an even greater extent.

D. The Clear and Present Risks and Resulting Impact on Customers

14. The alleged harms described herein are not speculative and pose real danger to all of the Members, individuals and entities alike wherever they are located. In the crypto environment, and amidst the current hype and media interest surrounding cryptocurrencies, coupled with the clear and present danger posed by hackers, disclosure of the Members' names would inevitably be subjected to intense scrutiny and investigative stalking, media publicity and likely unjustifiable media intrusion (of both themselves as well as their family, friends and colleagues)—in addition to the real risk posed by crypto hackers, SIM swapping, physical robbery, theft of private crypto keys, online wallet theft and daily attacks on their accounts through ransomware, blackmail, fraud, phishing and/or viruses. Moreover, publishing the names of Member entities, in effect, creates a list of potential targets for thieves to target. Sophisticated criminals can rely on numerous publicly available platforms (*i.e.*, LinkedIn, etc.) to obtain information relative to the Member entity's employees, directors, or others associated with the entity. Criminals can then target these individuals using the same methods discussed above in Paragraph 10, *supra*. This subjects Member entities to an undue risk of unlawful injury.

15. In short, distress, anxiety, and loss of privacy (non-pecuniary losses) as well as economic losses may well be suffered as a result of these real risks—all of which are types of

losses that are recoverable under GDPR and associated privacy laws (aside and separate to the fines and sanctions that may be brought by the supervisory authorities under GDPR).[2]

16. In the present case, it seems there is an important distinction to be made between personal information being disclosed to a specific entity for a specific purpose and for a limited duration in contrast to widespread public dissemination of this same information, which would otherwise result in infinite, unlimited and unrestricted use and therefore no longer be subject to the Court's control.

17. Whilst not being a US qualified lawyer, there is considerable evidence that demonstrates the public interest in disclosing the names of Members is outweighed by the real and

---

[2] In this context, we'd specifically also like to draw the court's attention to the recent 22 November 2022 EU decision in *Joined Cases C-37/20* and *C-601/20 WM (C-37/20) and Sovim SA (C-601/20) v Luxembourg Business Registers*, in which the Court of Justice of the European Union ("CJEU") determined in a preliminary ruling that the general public's access to information on beneficial ownership constitutes a serious interference with the fundamental rights to respect for private life and to the protection of personal data, enshrined in Articles 7 and 8 of the EU Charter.

The CJEU held that the provision of the anti-money-laundering directive, whereby Member States must ensure that the information on the beneficial ownership of corporate and other legal entities incorporated within their territory is accessible in all cases to any member of the general public, is invalid. According to the CJEU, the general public's access to information on beneficial ownership constitutes a serious interference with the fundamental rights to respect for private life and to the protection of personal data under the Charter. The CJEU noted that making the information publicly available enables a potentially unlimited number of persons to find out about the material and financial situation of the beneficial owner. The information also can be retained and disseminated by anyone who accesses it, which, according to the CJEU, increases the potential abuse of the information.

In its decision, the CJEU clarified that the EU legislature is pursuing an objective general interest with regard to the anti-money-laundering directive (*i.e.* seeking to prevent money laundering and terrorist financing), and that an objective interest is capable of justifying interferences with the fundamental rights of the Charter. However, the CJEU went on to hold that the interference entailed by making the information publicly accessible is neither limited to what is strictly necessary, nor proportionate to the objective pursued.

The decision can be found at: https://curia.europa.eu/juris/document/document.jsf?text=beneficial%2Bownership%2B&docid=268059&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=48841#ctx1.

likely risk to the Members' privacy, livelihood, private life and financial wellbeing.

18. It is for these reasons that, in my view, the Motion should be granted.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on March 17, 2023, at London, United Kingdom.

/s/Philip James
Philip James